

WHITEPAPER

# **EU-Regulierung als Wettbewerbsvorteil**

Am Beispiel von DORA und NIS-2

*Ein Leitfaden für kleine und mittelständische Unternehmen*

Autor:

Dipl. Wirtschaftinf. (FH) Christian Nass  
mit freundlicher Unterstützung von Opus 4.5

Stand: Januar 2026

## Management Summary

Die Digitalisierung und zunehmende Vernetzung von Geschäftsprozessen stellen kleine und mittelständische Unternehmen (KMU) vor neue Herausforderungen – aber auch vor erhebliche Chancen. Mit dem Digital Operational Resilience Act (DORA) und der NIS-2-Richtlinie hat die Europäische Union zwei wegweisende Regelwerke geschaffen, die Cybersicherheit und digitale Widerstandsfähigkeit zur Chefsache machen.

Dieses Whitepaper zeigt, warum proaktives Handeln bei der Umsetzung dieser Regularien nicht nur vor Sanktionen schützt, sondern einen echten Wettbewerbsvorteil darstellt. Unternehmen, die frühzeitig in IT-Sicherheit investieren, stärken das Vertrauen von Kunden und Geschäftspartnern und positionieren sich als verlässliche Partner in einem zunehmend regulierten Marktumfeld.

### Die wichtigsten Fakten auf einen Blick:

- DORA gilt seit dem 17. Januar 2025 – ohne Übergangsfrist
- NIS-2 ist in Deutschland seit dem 6. Dezember 2025 in Kraft
- Über 30.000 Unternehmen in Deutschland sind von NIS-2 betroffen
- Bußgelder bis zu 10 Mio. Euro oder 2% des weltweiten Jahresumsatzes möglich
- Persönliche Managerhaftung bei Verstößen ausdrücklich vorgesehen

# 1. DORA – Digital Operational Resilience Act

## Was ist DORA?

Der Digital Operational Resilience Act (DORA) ist eine EU-Verordnung, die seit dem 17. Januar 2025 unmittelbar anwendbares Recht in allen EU-Mitgliedstaaten darstellt. DORA schafft einen einheitlichen Rahmen für das Management von IKT-Risiken (Informations- und Kommunikationstechnologie) im Finanzsektor und stellt sicher, dass Finanzunternehmen auch bei schwerwiegenden IT-Störungen oder Cyberangriffen handlungsfähig bleiben.

## Wer ist betroffen?

DORA richtet sich primär an:

- Banken und Kreditinstitute
- Versicherungsunternehmen
- Investmentgesellschaften und Zahlungsdienstleister
- FinTech-Unternehmen
- IKT-Drittanbieter (z.B. Cloud-Dienstleister, IT-Dienstleister für den Finanzsektor)

**Wichtig für KMU:** Auch kleinere Finanzunternehmen und IT-Dienstleister, die für Finanzunternehmen arbeiten, fallen unter DORA. Das **Verhältnismäßigkeitsprinzip** erlaubt jedoch angepasste Anforderungen je nach Unternehmensgröße.

## Die fünf Kernbereiche von DORA

Bereich	Beschreibung
<b>IKT-Risikomanagement</b>	Aufbau eines robusten Rahmens zur Identifikation, Bewertung und Steuerung von IT-Risiken
<b>Incident-Management</b>	Strukturierte Prozesse zur Erkennung, Meldung und Behandlung von Sicherheitsvorfällen
<b>Resilienztests</b>	Regelmäßige Tests inkl. Penetrationstests zur Überprüfung der Widerstandsfähigkeit
<b>Drittparteien-Management</b>	Überwachung und vertragliche Absicherung von IKT-Dienstleistern
<b>Informationsaustausch</b>	Freiwilliger Austausch von Bedrohungsinformationen zwischen Unternehmen

## 2. NIS-2 – Network and Information Security Directive

### Was ist NIS-2?

Die NIS-2-Richtlinie (Network and Information Security Directive 2) ist die Nachfolgerin der ursprünglichen NIS-Richtlinie aus dem Jahr 2016. Sie wurde am 6. Dezember 2025 in Deutschland durch das NIS-2-Umsetzungsgesetz in nationales Recht überführt und ist damit verbindlich anzuwenden.

NIS-2 verfolgt das Ziel, ein hohes gemeinsames Cybersicherheitsniveau in der gesamten EU zu erreichen. Im Vergleich zur Vorgängerrichtlinie erweitert NIS-2 den Anwendungsbereich erheblich und verschärft die Anforderungen an Risikomanagement und Meldepflichten.

### Wer ist betroffen?

NIS-2 betrifft in Deutschland schätzungsweise über 30.000 Unternehmen – deutlich mehr als die ca. 4.500 unter der Vorgängerrichtlinie. Betroffen sind Unternehmen in folgenden Sektoren:

Wesentliche Einrichtungen (Essential)	Wichtige Einrichtungen (Important)
<ul style="list-style-type: none"><li>• Energie</li><li>• Verkehr/Transport</li><li>• Banken</li><li>• Finanzmarktinfrastruktur</li><li>• Gesundheitswesen</li><li>• Trinkwasser</li><li>• Abwasser</li><li>• Digitale Infrastruktur</li><li>• Öffentliche Verwaltung</li><li>• Weltraum</li></ul>	<ul style="list-style-type: none"><li>• Post- und Kurierdienste</li><li>• Abfallbewirtschaftung</li><li>• Chemie</li><li>• Lebensmittel</li><li>• Verarbeitendes Gewerbe</li><li>• Digitale Dienste</li><li>• Forschung</li></ul>

**Größenkriterien:** In der Regel sind mittelgroße Unternehmen ab 50 Mitarbeitern oder mit einem Jahresumsatz von über 10 Mio. Euro betroffen. Unternehmen in besonders kritischen Bereichen können jedoch unabhängig von ihrer Größe erfasst sein.

### Kernanforderungen der NIS-2

1. **Risikomanagement:** Einführung eines Informationssicherheitsmanagementsystems (ISMS)
2. **Meldepflichten:** Erhebliche Sicherheitsvorfälle müssen innerhalb von 24 Stunden gemeldet werden
3. **Notfall-Management:** Backup- und Wiederherstellungspläne sowie Krisenmanagement
4. **Lieferkettensicherheit:** Sicherheitsanforderungen an Zulieferer und Dienstleister
5. **Schulungen:** Regelmäßige Cybersicherheits Schulungen für Mitarbeiter und Management
6. **Registrierung:** Betroffene Unternehmen müssen sich beim BSI registrieren

### 3. DORA und NIS-2 im Zusammenspiel

Obwohl beide Regelwerke ähnliche Ziele verfolgen – nämlich die Stärkung der Cybersicherheit und digitalen Resilienz – unterscheiden sie sich in wesentlichen Punkten:

Kriterium	DORA	NIS-2
Rechtsform	EU-Verordnung (direkt anwendbar)	EU-Richtlinie (nationale Umsetzung erforderlich)
Fokus	Finanzsektor	Branchenübergreifend (18 Sektoren)
Inkrafttreten	17. Januar 2025	6. Dezember 2025 (DE)
Max. Bußgeld	Bis 5 Mio. Euro; für IKT-Dienstleister: 1% des Tagesumsatzes	Bis 10 Mio. Euro oder 2% des weltweiten Umsatzes
Managerhaftung	Ja, ausdrücklich vorgesehen	Ja, persönliche Haftung der Geschäftsleitung

**Wichtig:** DORA gilt als Lex Specialis für den Finanzsektor. Das bedeutet: Finanzunternehmen, die DORA unterliegen, sind von bestimmten NIS-2-Anforderungen befreit, müssen aber in Bereichen, die DORA nicht abdeckt, dennoch die NIS-2-Vorgaben erfüllen.

## 4. Regulierung als Wettbewerbsvorteil

Die Umsetzung von DORA und NIS-2 erfordert zunächst Investitionen in IT-Sicherheit, Prozesse und Personal. Doch diese Investitionen zahlen sich mehrfach aus:

### Vertrauensvorsprung bei Kunden und Partnern

In einer Zeit zunehmender Cyberangriffe und Datenschutzskandale wird nachweisbare IT-Sicherheit zum Differenzierungsmerkmal. Unternehmen, die die strengen EU-Vorgaben erfüllen, **signalisieren Professionalität und Verlässlichkeit**. Dies ist besonders relevant in Geschäftsbeziehungen, in denen sensible Daten ausgetauscht werden oder kritische Prozesse ausgelagert sind.

### Zugang zu regulierten Märkten

Als IT-Dienstleister oder Zulieferer für regulierte Branchen (Finanzsektor, kritische Infrastrukturen, Gesundheitswesen) ist die Erfüllung von DORA- und NIS-2-Anforderungen zunehmend **Voraussetzung für Aufträge**. Wer die Anforderungen erfüllt, erschließt sich neue Geschäftsfelder.

### Reduzierung von Geschäftsrisiken

Die systematische Auseinandersetzung mit IT-Risiken und die Implementierung von Sicherheitsmaßnahmen reduzieren die Wahrscheinlichkeit erfolgreicher Cyberangriffe. Die durchschnittlichen **Kosten eines Datenlecks** liegen in Deutschland bei **über 4 Millionen Euro** – eine Investition in Prävention ist wirtschaftlich sinnvoll.

### Bessere Versicherungskonditionen

Cyberversicherungen werden angesichts steigender Schadensfälle teurer und selektiver. Unternehmen mit nachweisbar hohem Sicherheitsniveau erhalten **bessere Konditionen** oder überhaupt erst Zugang zu entsprechendem **Versicherungsschutz**.

*Cybersicherheit ist kein notwendiges Uebel, sondern ein Wettbewerbsvorteil. Wer frühzeitig in IT-Sicherheit investiert, gewinnt nicht nur regulatorische Sicherheit, sondern stärkt auch das Vertrauen von Kunden und Partnern.*

## 5. Praktische Umsetzungshinweise für KMU

### Schritt 1: Betroffenheitsprüfung

Klären Sie zunächst, ob Ihr Unternehmen von DORA und/oder NIS-2 betroffen ist:

- Nutzen Sie die Betroffenheitsprüfung des BSI (online verfügbar)
- Prüfen Sie, ob Sie als Zulieferer für regulierte Unternehmen tätig sind
- Im Zweifel: Holen Sie rechtliche Beratung ein

### Schritt 2: Gap-Analyse

Ermitteln Sie den Status quo Ihrer IT-Sicherheit:

- Nutzen Sie den kostenlosen CyberRisiko-Check nach DIN SPEC 27076
- Identifizieren Sie Lücken zwischen Ist-Zustand und gesetzlichen Anforderungen
- Priorisieren Sie Handlungsbedarfe nach Risiko und Aufwand

### Schritt 3: ISMS aufbauen

Ein Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001 bildet eine solide Grundlage:

- Definieren Sie klare Verantwortlichkeiten (Informationssicherheitsbeauftragter)
- Erstellen Sie Richtlinien für IT-Sicherheit, Zugriffsmanagement, Backup etc.
- Führen Sie regelmäßige Risikoanalysen durch

### Schritt 4: Technische Maßnahmen umsetzen

- Netzwerksegmentierung und Firewall-Konfiguration
- Multi-Faktor-Authentifizierung für kritische Systeme
- Regelmäßige Backups mit getesteter Wiederherstellung
- Patch-Management und zeitnahe Sicherheitsupdates
- Verschlüsselung sensibler Daten

### Schritt 5: Meldeprozesse etablieren

- Definieren Sie, wann ein Vorfall meldepflichtig ist
- Richten Sie Prozesse für die fristgerechte Meldung ein (24 Stunden!)
- Benennen Sie verantwortliche Ansprechpartner

### Schritt 6: Schulung und Sensibilisierung

- Schulen Sie alle Mitarbeiter regelmäßig zu Cybersicherheit
- Die Geschäftsleitung muss an Schulungen teilnehmen (gesetzliche Pflicht!)
- Führen Sie Phishing-Simulationen und Awareness-Kampagnen durch

## 6. Checkliste für die Umsetzung

✓	Maßnahme
<input type="checkbox"/>	Betroffenheit nach DORA und/oder NIS-2 geprüft
<input type="checkbox"/>	Verantwortlichkeiten auf Geschäftsleitungsebene festgelegt
<input type="checkbox"/>	Gap-Analyse durchgeführt
<input type="checkbox"/>	Risikomanagementprozess etabliert
<input type="checkbox"/>	Sicherheitsrichtlinien dokumentiert
<input type="checkbox"/>	Technische Schutzmaßnahmen implementiert
<input type="checkbox"/>	Backup- und Notfallpläne erstellt und getestet
<input type="checkbox"/>	Meldeprozesse für Sicherheitsvorfälle definiert
<input type="checkbox"/>	Mitarbeiterschulungen durchgeführt
<input type="checkbox"/>	Management-Schulungen absolviert
<input type="checkbox"/>	Drittanbieter-Risiken bewertet und vertraglich abgesichert
<input type="checkbox"/>	Registrierung beim BSI erfolgt (für NIS-2)
<input type="checkbox"/>	Regelmäßige Überprüfung und Aktualisierung geplant

## 7. Fazit

DORA und NIS-2 markieren einen Paradigmenwechsel in der europäischen Cybersicherheitsregulierung. Die neuen Anforderungen sind anspruchsvoll – aber sie bieten KMU auch strategische Chancen:

- ✓ Frühzeitiges Handeln verschafft Wettbewerbsvorteile gegenüber Mitbewerbern
- ✓ Nachweisbare Compliance öffnet Türen zu regulierten Märkten und Kunden
- ✓ Investitionen in IT-Sicherheit sind Investitionen in Geschäftskontinuität
- ✓ Strukturierte Prozesse reduzieren Risiken und schaffen Handlungssicherheit im Krisenfall

Die Umsetzung sollte nicht als reine Pflichtaufgabe verstanden werden, sondern als Investition in Wettbewerbsfähigkeit und Resilienz. Entscheidend ist, jetzt zu handeln: Die regulatorischen Anforderungen gelten bereits, und die Aufsichtsbehörden werden die Einhaltung aktiv prüfen.

### **Handeln Sie jetzt!**

Beginnen Sie heute mit der Betroffenheitsprüfung und planen Sie Ihre Compliance-Roadmap. Die Zeit drängt – aber mit einem strukturierten Ansatz ist die Umsetzung auch für KMU machbar.

## **Weiterführende Ressourcen**

### **Offizielle Quellen**

- BSI – Bundesamt für Sicherheit in der Informationstechnik: [www.bsi.bund.de](http://www.bsi.bund.de)
- BaFin – Bundesanstalt für Finanzdienstleistungsaufsicht: [www.bafin.de/dora](http://www.bafin.de/dora)
- NIS-2-Betroffenheitsprüfung des BSI: [betroffenheitspruefung.bsi.bund.de](http://betroffenheitspruefung.bsi.bund.de)

### **Standards und Normen**

- ISO/IEC 27001 – Informationssicherheitsmanagementsystem
- DIN SPEC 27076 – CyberRisiko-Check für KMU
- BSI IT-Grundschatz

### **Unterstützungsangebote**

- IHK – Industrie- und Handelskammern: Kostenlose Erstberatung und Seminare
- Mittelstand-Digital: Förderprogramme und Kompetenzzentren
- Allianz für Cyber-Sicherheit des BSI

*Hinweis: Dieses Whitepaper dient der allgemeinen Information und ersetzt keine rechtliche oder fachliche Beratung im Einzelfall. Stand der Informationen: Januar 2026.*